Abstract on

**PSEUDO RANDOM SEQUENCE GENERATOR**

Submitted by

Advaith Auron S.

Manikandan V.

Ravishankar S. R

**Abstract:**

The aim of this project is to generate pseudo-random sequences using atmospheric noise. A pseudorandom number generator (PRNG), also known as a deterministic random bit generator (DRBG) is an algorithm for generating a sequence of numbers that approximates the properties of random numbers. The sequence is not truly random in that it is completely determined by a relatively small set of initial values, called the PRNG's state, which includes a truly random seed. A linear Congruential generator is used for generating PRNG. A Linear Congruential Generator (LCG) represents one of the oldest and best-known pseudorandom number generator algorithms.  The generator is defined by the [recurrence relation](http://en.wikipedia.org/wiki/Recurrence_relation):

X_{n+1} \equiv \left( a X_n + c \right)~~\pmod{m}

Where X is the [sequence](http://en.wikipedia.org/wiki/Sequence) of pseudorandom values, and

 m,\, 0<m — The "modulus"

 a,\,0 < a < m— The "multiplier"

 c,\,0 \le c < m— The "increment"

 X_0,\,0 \le X_0 < m— The "seed" or "start value"

are [integer](http://en.wikipedia.org/wiki/Integer) constants that specify the generator. It is known that the atmospheric noise is truly random hence if we sample the noise, the samples will also be random in nature. The values to be fed to the variable Xn is obtained by sampling the atmospheric noise. Atmospheric noise is radio noise caused by natural atmospheric processes, primarily lightning discharges in thunderstorms. The sum of all these lightning flashes results in atmospheric noise. It can be observed with a radio receiver in the form of a combination of [white noise](http://en.wikipedia.org/wiki/White_noise) (coming from distant thunderstorms) and [impulse noise](http://en.wikipedia.org/wiki/Impulse_noise) (coming from a near thunderstorm). Although lightning has a broad-spectrum emission, its noise power increases with decreasing frequency. Therefore, at [very low frequency](http://en.wikipedia.org/wiki/Very_low_frequency) and [low frequency](http://en.wikipedia.org/wiki/Low_frequency), atmospheric noise often dominates. So, a low frequency AM receiver is used to receive the noise. Now the samples obtained from atmospheric noise is used as the seed (Xn) in the LCG. The coding is done using any standard program like MATLAB or SCILAB. The sequence obtained at the output of the LCG is checked for the properties of random numbers. The sequence is tested for two basic properties of randomness-uniformity and independence using various tests to obtain a sequence with excellent quality.